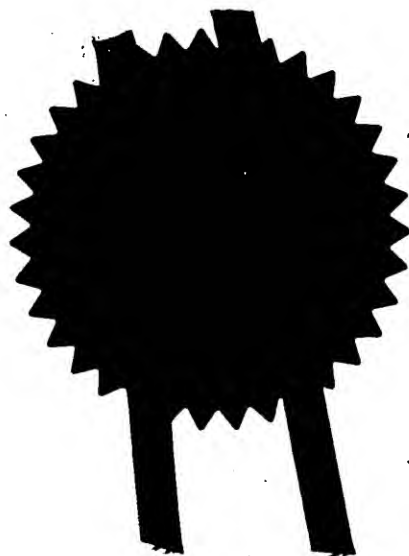The Patent Office

INVESTOR IN PEOPLE

The Patent Office
Concept House
Cardiff Road
Newport
South Wales
NP10 8QQ

I, the undersigned, being an officer duly authorised in accordance with Section 74(1) and (4) of the Deregulation & Contracting Out Act 1994, to sign and issue certificates on behalf of the Comptroller-General, hereby certify that annexed hereto is a true copy of the documents as originally filed in connection with the patent application identified therein.

In accordance with the Patents (Companies Re-registration) Rules 1982, if a company named in this certificate and any accompanying documents has re-registered under the Companies Act 1980 with the same name as that with which it was registered immediately before re-registration save for the substitution as, or inclusion as, the last part of the name of the words "public limited company" or their equivalents in Welsh, references to the name of the company in this certificate and any accompanying documents shall be treated as references to the name with which it is so re-registered.

In accordance with the rules, the words "public limited company" may be replaced by p.l.c., plc, P.L.C. or PLC.

Re-registration under the Companies Act does not constitute a new legal entity but merely subjects the company to certain additional company law rules.
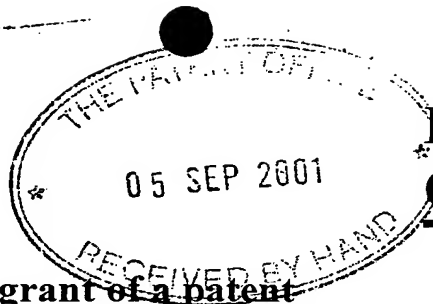
Signed

Dated   12 FEB 2002

CERTIFIED COPY OF PRIORITY DOCUMENT

An Executive Agency of the Department of Trade and Industry

05 SEP 2001

The Patent Office

06SEP01 E657815-03 001038
_F01/7700 0.00-0121502.9

1/77

Request for grant of a patent

(See the notes on the back of this form. You can also get an explanatory leaflet from the Patent Office to help you fill in this form)

05 SEP 2001

The Patent Office
Cardiff Road
Newport
South Wales
NP10 8QQ

1. Your reference	P103206GB/SAB/47108

2. Patent application number *(The Patent Office will fill in this part)*	**0121502.9**

3. Full name, address and postcode of the or of each applicant *(underline all surnames)*	Data Encryption Systems Limited Silver Street House Silver Street Taunton Somerset TA1 3DL
Patents ADP number *(if you know it)*	8220170001
If the applicant is a corporate body, give the country/state of its incorporation	England

4. Title of the invention	APPARATUS FOR AND METHOD OF CONTROLLING PROPAGATION OF DECRYPTION KEYS

5. Name of your agent *(if you have one)*	
"Address for service" in the United Kingdom to which all correspondence should be sent *(including the postcode)*	WITHERS & ROGERS Goldings House 2 Hays Lane London SE1 2HW
Patents ADP number *(if you know it)*	1776001

6. If you are declaring priority from one or more earlier patent applications, give the country and the date of filing of the or each of these earlier applications and *(if you know it)* the or each application number	Country	Priority application number *(if you know it)*	Date of filing *(day / month / year)*
	---		

7. If this application is divided or otherwise derived from an earlier UK application, give the number and the filing date of the earlier application	Number of earlier application	Date of filing *(day / month / year)*
	---	

8. Is a statement of inventorship and of right to grant of a patent required in support of this request? *(answer 'Yes' if:* *a) any applicant named in part 3 is not an inventor, or* *b) there is an inventor who is not named as an applicant, or* *c) any named applicant is a corporate body.* *See note (d))*	YES

9. Enter the number of sheets for any of the
   following items you are filing with this form.
   Do not count copies of the same document

Continuation sheets of this form

Description 9

Claim(s) 3

Abstract 1

Drawing (s) 5

10. If you are also filing any of the following, state
    how many against each item.

Priority documents --

Translations of priority documents --

Statement of inventorship and --
right to grant of a patent *(Patents Form 7/77)*

Request for preliminary examination 1
and search *(Patents Form 9/77)*

Request for substantive examination 1
(Patents Form 10/77)

Any other documents --
(please specify)

11.

I/We request the grant of a patent on the basis of this application.

Signature *W. Heist Rogers* Date

WITHERS & ROGERS 4th September 2001

12. Name and daytime telephone number of   Simon A Beck   0117 925 3030
    person to contact in the United Kingdom

Warning
*After an application for a patent has been filed, the Comptroller of the Patent Office will consider whether publication or
communication of the invention should be prohibited or restricted under Section 22 of the Patents Act 1977. You will be
informed if it is necessary to prohibit or restrict your invention in this way. Furthermore, if you live in the United Kingdom,
Section 23 of the Patents Act 1977 stops you from applying for a patent abroad without first getting written permission from the
Patent Office unless an application has been filed at least six weeks beforehand in the United Kingdom for a patent for the same
invention and either no direction prohibiting publication or communication has been given, or any such direction has been
revoked.*

Notes
a)   If you need help to fill in this form or you have any questions, please contact the Patent Office on 0645 500 505.
b)   Write your answers in capital letters using black ink or you may type them.
*c)   If there is not enough space for all the relevant details on any part of this form, please continue on a separate sheet of
      paper and write "see continuation sheet" in the relevant part(s). Any continuation sheet should be attached to this form.*
d)   If you have answered 'Yes' Patents Form 7/77 will need to be filed.
e)   Once you have filled in the form you must remember to sign and date it.
f)   For details of the fee and ways to pay please contact the Patent Office.

P103206GB

APPARATUS FOR AND METHOD OF CONTROLLING PROPAGATION OF DECRYPTION KEYS

The present invention relates to an apparatus for and a method of controlling propagation of decryption keys or access to encrypted information.

There is often a need to control access to data. In some computing environments this goal has been achieved by virtue of limiting the physical access to a machine, to a data carrier, or to parts of a local area network. However such systems can be unnecessarily rigid and cumbersome, especially when the class of persons to whom access may be allowed or denied to a particular item of data is ill defined.

Another approach to security is the use of encryption. In a secure system, the identities of the or each person who should have access to a document or other item of encrypted data needs to be defined at the time of encryption. This can, once again, be difficult where the class of people who should receive the data is ill defined.

Neither of these themes works particularly well in a "generally trusted" environment where absolute security is not necessary. An example of a generally trusted environment is a company where a manager may be dealing with a commercially sensitive document, and may wish to share this with other managers and in turn recognises that they may need to share the document with other individuals where they deem this to be necessary or desirable. Thus the document cannot be "open" such that everyone can view it, as it may be commercially sensitive, but neither can the recipient list be accurately defined right from the outset.

According to a first aspect of the present invention, there is provided a security system for controlling access to encrypted information, the security system comprising a hardware device for storing a decryption key for use in decrypting an encrypted item of information, the decryption key being associated with the security code which is used by the hardware device to determine whether it is authorised to send encrypted copies of the decryption key to others.

It is thus possible to give the originator of an item of information control over the number of times that that item of information may be passed from one person to another or how many times the decryption key can be passed from one person to another, under circumstances where the item of information is in an encrypted form.

Preferably the decryption key is related to a specific project or task. Thus the controller or originator of a task can generate a key which can be used for encryption and decryption of documents within that project or task.

Advantageously the decryption key may also include a further identifier which is unique to an entity, such as a company, so that only people having a corresponding code portion in their security device can decrypt the key for the documents.

Preferably, when a further person wishes to receive a copy of the encrypted information, the decryption key for the encrypted information is sent to that other user in an encrypted form. Advantageously the encryption key is itself encrypted with the recipient's public encryption key.

Advantageously the hardware device further modifies the security code each time it sends the decryption key to another user. It is thus possible to keep a track on the number of times the decryption key is propagated from one person to another. This security code may, for example, be a "generation limit" set by the originator of the document, and each time the decryption key is propagated, the generation limit is decremented. Once the generation limit reaches zero, further propagation of the decryption key is inhibited by the hardware device.

Advantageously the decryption key is further associated with a security device and/or user identity number which is unique. Each time the decryption key is propagated, the identity of the user or security device which authorised the propagation of the decryption key may be added to the decryption key. It is thus possible for an audit trail to be identified which shows the path through which a decryption key has passed. The identity may overwrite a previous identity or be appended to a list of identities. The list may be stored in the security device or elsewhere, such as a log file in a user's computer.

Advantageously, when propagating a decryption key to a further user, the person authorising the propagation may have the ability to modify the generation limit, so as to decrement it. A person authorising the propagation of the key, or the originator, may also be able to set one or more control words or control flags such that the security device is instructed to send a message to that person when an attempt to further propagate the key is initiated. Indeed, the further propagation of the decryption key may be inhibited until such time as that person sends a return message to the security device authorising the further propagation of key. Thus it is possible to set the security system such that it automatically generates an audit trail and/or such that it seeks further authority from a manager when sending further copies of the decryption key, which copies still represent "generations" of the key which are within the limit authorised by the "generation limit".

The authority to send the key may be generated automatically by an agent on a server which keeps a control log of propagations.

The security device may interface with a further device permanently embedded within the computer, or software loaded or embedded within the computer such that attempts to access a secure document without the proper decryption key results in a message being sent back to a system administrator, or the author of the document, or some other person defined by a suitable security field included within the document or included within a security file associated with the document. The file associated with the document may itself be encrypted.

Advantageously the security device is in the form of a small unit which the user can carry with them and which is dockable and undockable with a data processor, for example a standard PC, portable computing device and so on having a suitable socket. Thus, the security device effectively functions as a dongle, but is not to be confused with the old style dongles which were hardware devices permanently connected to the printer port of a computer. Wireless communication is also possible.

The security device may be password protected. Advantageously it can be set to disable after a number of incorrect entries of the password.

According to a second aspect of the present invention, there is provided a method of controlling access to of encrypted data, the method comprising encrypting the data with an encryption key, and making copies of the decryption key available to selected persons, the decryption keys being associated with a propagation control word, and wherein in response to an instruction to send the decryption key to a specified recipient, the propagation control word is checked to determine whether the propagation of the decryption key is allowed, and if so the control word is modified and then the decryption key and the control word are encrypted with the recipient's public key and sent to the recipient.

Advantageously the control word is set by an originator of the encrypted data and the control word is decremented at each propagation, with further propagation of the decryption key being inhibited once the control word reaches a predetermined value. The predetermined value may, for example, be zero.

Preferably each recipient of the key has the ability to modify the control word such that the number of further propagations can be reduced, but not increased.

Encryption and decryption keys can belong to individuals, or can belong to groups of people such that data can be shared amongst those people working, for example, on a particular project.

The hardware component of the system preferably includes a data processor such that encryption and decryption of the decryption key is performed solely within the hardware unit. Additionally the hardware unit may further comprise a non-volatile memory such that the association between an encrypted document or other entity or service and the appropriate decryption key is maintained solely within the hardware unit.

It is thus possible to provide a security system which allows limited propagation of an encrypted document or access thereto, even in an environment where the group of recipients requiring access to that document is not well defined.

The present invention will further be described, by way of example, with reference to the accompanying drawings, in which:

Figure 1 schematically illustrates a possible propagation path for a sensitive document within a multi-user environment;

Figure 2 schematically illustrates a user's computing device as modified to work within a security system constituting an embodiment of the present invention;

Figure 3 schematically illustrates the structure of a hardware security device constituting an embodiment of the present invention;

Figure 4 schematically illustrates the structure of a decryption key associated with a document in a security system constituting an embodiment of the present invention; and

Figure 5a and 5b represents a flow chart illustrating the operation of a security system constituting an embodiment of the present invention.

Figure 1 illustrates the arrangement where a originator 2 of a document wishes or needs to share this document with his co-workers 4 and 6. However, for whatever reason, the originator 2 may desire that the document does not reach his colleague 8. However, since workers 4 and 6 have had access to the document, they may then deal with it as they see fit, and worker 6 may for example forward the document on to a further colleague 10 who unaware of the wishes of the originator 2 may then forward the document on to the worker 8. The worker 6 may also e-mail the document to another person 12 via an external telecommunications network 14. Thus the contents of the document have now escaped from the control of the originator and the document may circulate amongst other people outside of the company.

A traditional way to address this problem would be to encrypt the document at the time of transmission to workers 4 and 6. Depending on the security features of the encryption system used, the originator 2 may be able to inhibit further copying or printing of the document by workers 4 and 6. However, if worker 6 has a legitimate need to forward that document onto a colleague 10, then this is clearly inconvenient. However, if the document is encrypted but further copying is permitted, then there is nothing stopping worker 6 forwarding the document on to his colleague 10, who may then of course forward the document on to worker 8.

The inventor has noted that, each time the encrypted document is transmitted to a new recipient, or a person is to be given access to the document, folder to the like there is an opportunity to encrypt the decryption key using the recipient's public key. This gives an opportunity for a security system to monitor the number of times that the decryption key has been propagated and thereby control the level of propagation of the decryption key, and hence the ability to decrypt the encrypted document. Thus, in general terms, the originator of a document 2 may send the document or give access to recipients 4 and 6 and may also set a propagation control value to, for example, 1 thereby indicating that the decryption key can be propagated one more time. Thus, user 6 has the option to re-encrypt the decryption key using the public key of intended recipients to make one further generation copy of the decryption key. Thus, as the decryption key is encrypted with the public key of user 10, the generation (ie copy) control word as embedded in the decryption key sent to user 10 is decremented, such that the generation control key received by user 10 has a value of zero. Thus, although user 10 could still send the encrypted document to worker 8, he will not be able to send the decryption key to worker 8 and thus worker 8 is unable to view the document. Similarly, the user 6 still has the ability to send the key to user 12 as this still only represents a further one generation (copy) step on from user 6. However, the originator 2 may also be able to set a copy limit variable which limits the number of times the user 6 can send the decryption key to a next generation user. Thus, if for example the copy control word was set to one, and the generation control word as received by user 6 was set to one, then user 6 could send a further copy of the decryption key to recipient 10, but in so doing the copy control word stored within the security system belonging to user 6 would be decremented such that the ability of user 6 to send a further copy to user 12, even though this would still represent only one further generation of copying, would be inhibited because user 6 had made their quota of copies.

Thus, the originator of a key has the ability to control both the number of "generations" to which the decryption key may be copied and independently the number of times any key may be copied within a single generation, that is the number of times the user may send a key to others.

Figure 2 schematically illustrates a computer terminal within a security system constituting an embodiment of the present invention. The computer terminal, generally indicated 20 is

in many ways a conventional terminal, such as a standard PC, having a main unit 22 housing a data processor, semiconductor memory, and bulk storage memory, together with various interface cards enabling the computer to communicate with other data processors via a suitable communications network 23 which may be a LAN, a WAN, a dial up connection or any other suitable communication scheme. The data processor also includes a display device 24 and an input device 26, for example a keyboard. A data processor also includes a socket 30 for removably accepting a user security device 32 such that the device 32 can establish data communication with the data processor 20.

The user's security device 32 is shown in greater detail in Figure 3. In broad terms, the device comprises an embedded data processor 34 connected via an internal bus 35 to a read only memory 36 containing the executable code for causing the microprocessor 34 to perform encryption and decryption operations and to check the generation and copy control words. The device 32 also includes a non-volatile memory 38 which contains decryption keys and associated identifiers and settings. It should be noted that the internal bus 35 is not directly accessible from outside of the device 32 but all communication is in fact handled via the data-processor 34. This prevents the memory 38 from being interrogated other than by the data-processor 34. Communication between the device 32 and the data processor 30 can be by a bespoke or via standard communications port. Thus, for computers produced around the years 2000 and 2001 the communication is likely to be via a USB interface. The interface can, of course, change dependent on the prevailing interface technology.

Figure 4 shows the configuration of data within the memory 38 in greater detail. The memory 38 is divided into a series of data units. A single data unit 40 is represented in Figure 4 and comprises a plurality of elements. A first element 50 is a serial number representing a unique identity of the key. A second portion 52 includes the copy control commands indicating either, or both the number of generations of copies which can be made of the decryption key (ie the number of tiers through which it may be copied from user to user), and indeed the number of copies that can be made within a single generation or more. Region 54 contains the decryption key itself and region 56 contains other data, such as the audit trail and any flags or other instructions which may for example concern the need to communicate with persons higher up a data flow path in order to authorise

further copying of the decryption key or to inform them that copying of the decryption key has been done.

Figures 5a and 5b schematically illustrate the operation of an embodiment of the present invention. Initially, control starts at step 70 where it is assumed that a user already has the encryption key, for example the public key, of a recipient which he wishes to send a decryption key to. From step 70, control is passed to step 72 where a test is made to see if the generation number is greater than zero. If the generation number is not greater than zero, then control is passed to step 74 where the procedure is exited. However, if the generation number is greater than zero then control is passed to step 76 where a test is made to see if a "group code flag" has been set. The group code is part of the recipient's public key which indicates which organisation they belong to. Thus, the group code can be examined and compared with a pass or deny list in order to determine whether the recipient is entitled to receive the decryption key. If the group code flag is set, control is passed to step 78, whereas if the flag is not set control is passed to step 82.

Step 78 compares the group code embedded in the key which the user wishes to send with the group code of the recipient. If the codes match, or lie within an acceptable range of codes, then control is passed to step 82, otherwise control is passed to step 80 where the procedure is terminated. An internal copy of the key which the user wishes to send is made at step 82 and control is then passed to step 84 where a test to see whether a copy control counter is set. If the copy control counter is set, then control is passed to step 86 whereas, if it is not, control is passed to step 94 as shown in Figure 5b.

A test is made at step 86 to see if the copy number is greater than zero. If it is not, then control is passed to step 88 where the procedure is exited. However, if the copy control number is greater than zero then control is passed to step 90 where the copy control number is decremented, and then to step 92 where the modified copy of the key including the decremented copy controlled number is rewritten back to the dongle. Control then proceeds to step 94 where the generation number is decremented, and then the modified generation number is merged with the key at step 96. From step 96, control is passed to step 98 where the key and modified generation and/or copy numbers are encrypted with the

recipients public key. Control is then passed to step 100 where the key is sent to the recipient. The procedure finishes at step 102.

The above system has been described in terms of allowing access to documents, but could equally apply to access to services, folders, executable files, web pages and so on. Thus one or more documents, some of which may not have yet been generated may be encrypted using the key and shared amongst users.

It would also be possible to use the system to control access to updates to a journal service or the like for a period of time.

Furthermore, although the invention has been described in the context of controlling the propagation of decryption keys, it is equally applicable to controlling the propagation of other security measures such as encryption keys, keys for encryption and decryption, passwords, messages and other electronic "objects" where the ability to propagate that "object" needs to be restricted.

It is thus possible to provide a security system for controlling the extent of propagation of keys.

CLAIMS

1. A security system for controlling access to encrypted information, comprising

a hardware device for storing at least one decryption key for use in decrypting an encrypted item of information the decryption key being associated with a security code which is used by the hardware device to determine whether it is authorised to send encrypted copies of the decryption key to others.

2. A security system as claimed in claim 1, in which, if the hardware device is authorised to send an encrypted copy of the decryption key to a first entity, it encrypts the decryption key using an encryption key associated with the first entity.

3. A security system as claimed in claim 2, in which the decryption key is encrypted with the public key of the first entity.

4. A security system as claimed in any one of the preceding claims, in which each time the hardware device sends a decryption key to another entity, it modifies the security code associated with the decryption key and sends the modified security code as part of the encrypted decryption key.

5. A security system as claimed in claim 4, in which the security code is a numeric value indicating the number of times the encryption key can be propagated, and the security code is decremented each time the decryption key is propagated to a further entity.

6. A security system as claimed in any one of the preceding claims in which the decryption key is stored within the hardware device.

7. A security system as claimed in any one of the preceding claims, in which the hardware device is removable from a data processor.

8. A security system as claimed in any one of the preceding claims, in which the hardware device is in the form of a user unit, which, in use, a user introduces to a data processor when the user wishes to use the data processor to access encrypted information and removes the user unit from the data processor when the user has finished.

9. A security system as claimed in any one of the preceding claims, in which each time the hardware device propagates a decryption key, it includes as part of the key an identifier indicating the identity of the sender's key.

10. A security system as claimed in claim 9, in which the decryption key includes an audit trail of individuals who have allowed propagation of the key.

11. A security system as claimed in claim 9 and 10, in which a user can append a control word against their identity in the decryption key to instruct the hardware device to initiate a message to them or an agent informing them of the propagation of the key and giving information concerning that propagation.

12. A security system comprising a plurality of hardware devices as claimed in any one of the preceding claims, and in which the decryption key is passed from hardware device to hardware device.

13. A security system as claimed in any one of the preceding claims, in which a user's private key is stored within their own hardware device, such that the encrypted decryption key can only be decrypted when the hardware device is in operation.

14. A security system as claimed in any of the preceding claims, wherein the hardware device includes a data processor such that all encryption and decryption of the decryption keys is performed within the hardware device.

15. A method of controlling the propagation of decryption keys for allowing access to encrypted data, comprising the steps of associating a propagation control word with a decryption key for an item of data, and in response to an instruction to send the key to a specified recipient, checking the status of the control word to determine if propagation is allowed, and if so, modifying the control word and encrypting the control word and decryption key with a recipient's public key and sending the encrypted key.

16. A method as claimed in claim 15, in which the control word is a numeric value which is decremented at each propagation, and in which propagation is inhibited once the numeric value reaches a predetermined value.

17. A method as claimed in claim 15 or 16, which the originator of a key sets the number of times the key can be sent, and each time a key is sent, a variable holding a generation number of the key is modified such that when the generation number reaches the maximum number of times the key can be sent, further sending of the key is inhibited.

13

ABSTRACT

APPARATUS FOR AND METHOD OF CONTROLLING PROPAGATION OF DECRYPTION KEYS

(Figure 5)

A encryption key propagation control system is provided in which a generation number (72) is identified with each decryption key and the generation number is queried each time a request is made to forward a decryption key to another user. The generation number is decremented at each request, and once it reaches a zero further requests are refused by the system.
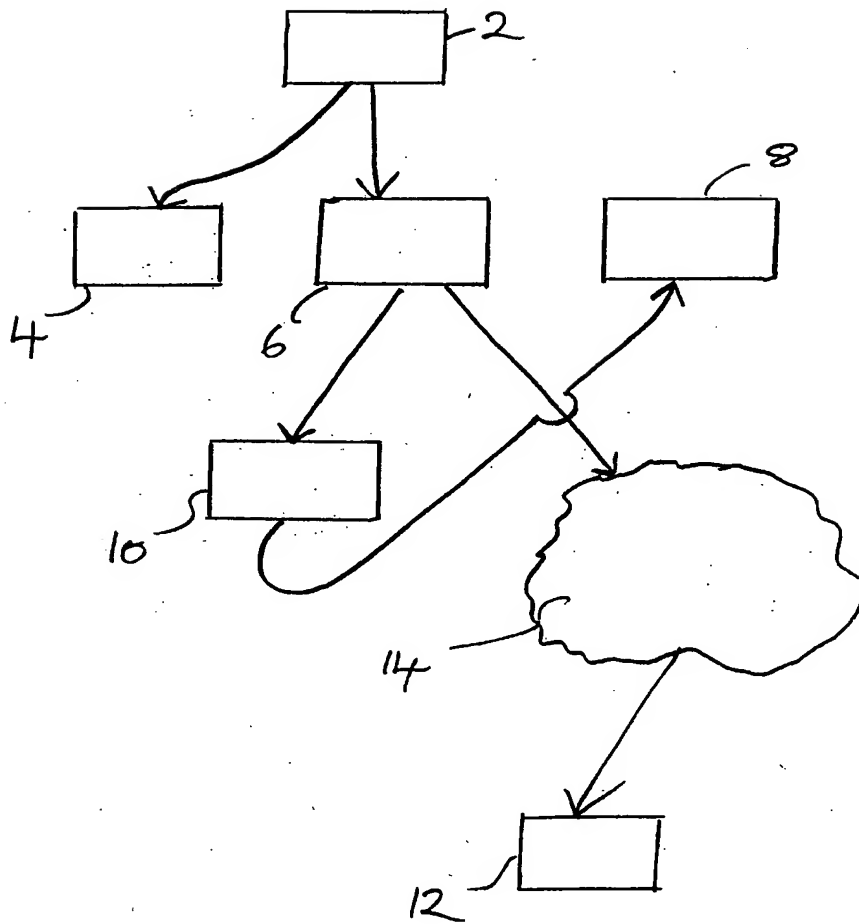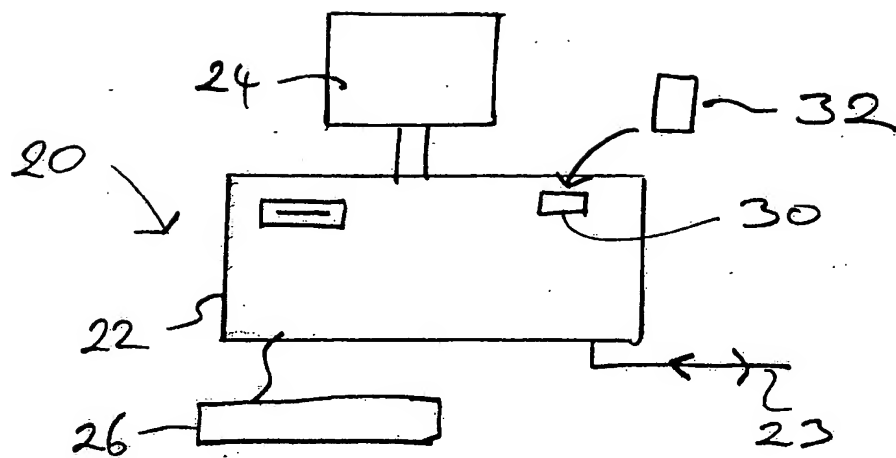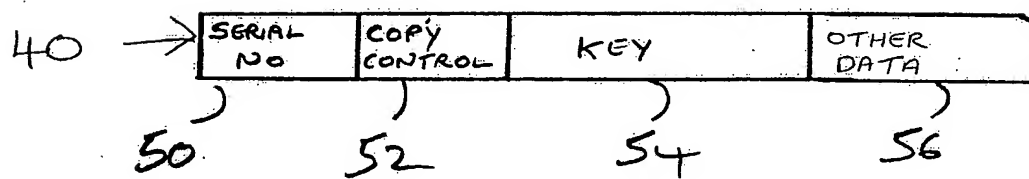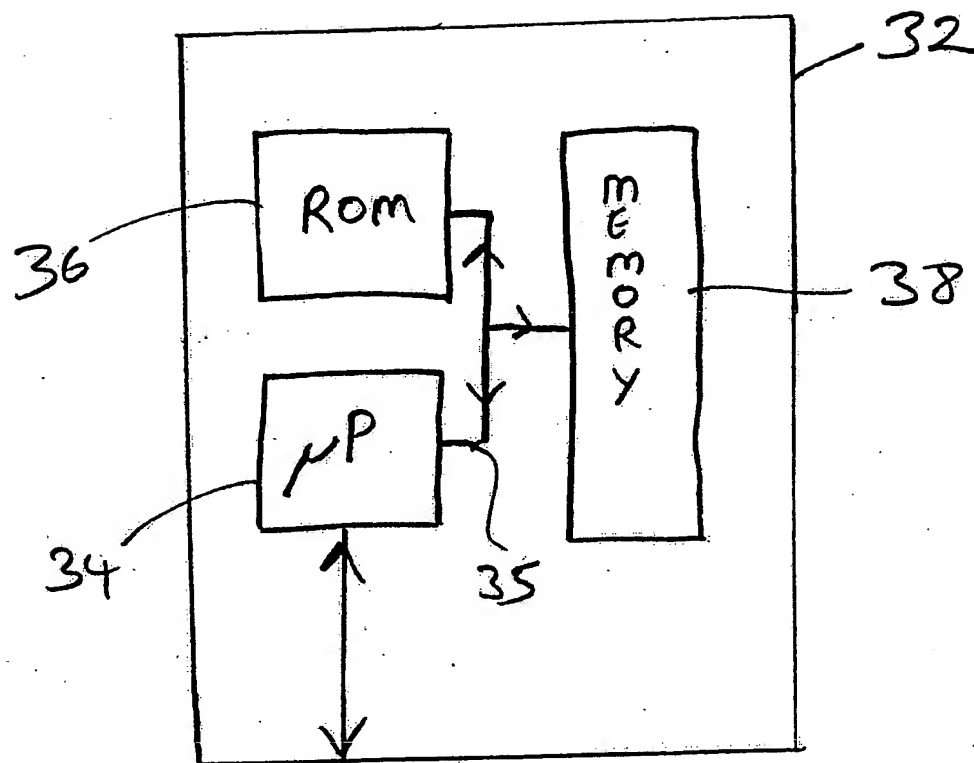
FIG.1

24

20

32

30

22

26

23

FIG.2

40

SERIAL NO	COPY CONTROL	KEY	OTHER DATA

50

52

54

56

FIG.4

32

ROM

36

μP

34

35

MEMORY

38

FIG.3

FIG.5a

B

IS COPY NO
> 0 — 86

N → EXIT — 88

Y

DECREMENT
COPY NO — 90

rewrite KEY
TO DONGLE — 92

A →

DECREMENT
GENERATION NO — 94

MERGE GENERATION
NO & KEY — 96

ENCRYPT WITH
RECIPIENT'S PUBLIC KEY — 9D

SEND KEY — 100

EXIT — 102

FIG.5b